

ÚSTAV EKOLÓGIE LESA SLOVENSKEJ AKADEMIE VIED, V. V. I.

INTERNÁ SMERNICA

o kybernetickej bezpečnosti

Vydavateľ:	Ústav ekológie lesa SAV, v. v. i.
Sídlo:	Štúrova 2, 960 53 Zvolen
IČO:	00679071
Číslo smernice:	2.4
Verzia:	1.0
Účinnosť od:	01. 07. 2026
Vypracoval:	Správca IT / Bezpečnostný manažér
Schválil:	Dozorná rada a Správna rada ÚEL SAV, v. v. i.
Právny základ:	Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti

Obsah

- Článok 1 – Úvodné ustanovenia a právny základ
- Článok 2 – Vymedzenie základných pojmov
- Článok 3 – Rozsah pôsobnosti a chránené priestory
- Článok 4 – Politika používania informačných technológií
- Článok 5 – Používanie hardvéru
- Článok 6 – Používanie softvéru
- Článok 7 – Používanie internetu a elektronickej pošty
- Článok 8 – Správa prístupov a hesiel
- Článok 9 – Zálohovanie a ochrana dát
- Článok 10 – Narušenie bezpečnosti a riešenie incidentov
- Článok 11 – Preventívne opatrenia
- Článok 12 – Práca s citlivými a osobnými dátami
- Článok 13 – Vzdelávanie a školenia
- Článok 14 – Kontrola a audit

Článok 15 – Záverečné ustanovenia

Príloha č. 1 – Žiadosť o pridelenie prístupu do IS

Príloha č. 2 – Záznam o bezpečnostnom incidente

Článok 1

Úvodné ustanovenia a právny základ

(1) Ústav ekológie lesa Slovenskej akadémie vied, verejná výskumná inštitúcia (ďalej len "ústav"), vydáva túto smernicu v súlade s nasledujúcou legislatívou:

- Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení neskorších predpisov,
- Zákon č. 95/2019 Z. z. o informačných technológiách vo verejnej správe,
- Smernica Európskeho parlamentu a Rady (EÚ) 2022/2555 (NIS2), transponovaná do slovenského práva,
- Vyhláška NBÚ č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

(2) Cieľom tejto smernice je zabezpečiť ochranu informačných systémov, sietí, zariadení a dát ústavu pred kybernetickými hrozbami, neoprávneným prístupom, únikom informácií a inými bezpečnostnými incidentmi.

(3) Ústav je povinný dodržiavať zásady kybernetickej bezpečnosti ako výskumná organizácia narábajúca s citlivými vedeckými dátami, osobnými údajmi zamestnancov a výsledkami výskumu financovaného z verejných zdrojov.

Článok 2

Vymedzenie základných pojmov

Na účely tejto smernice sa rozumie:

- Používateľ – každý zamestnanec ústavu, doktorand, externý spolupracovník alebo iná fyzická osoba, ktorej bol pridelený prístup k informačnému systému ústavu.
- Správca IT – zamestnanec poverený správou, údržbou a bezpečnosťou informačných technológií ústavu.
- Bezpečnostný manažér – osoba zodpovedná za kybernetickú bezpečnosť; môže ísť o totožnú osobu so správcom IT alebo externú osobu.
- Informačný systém (IS) – súbor hardvérových a softvérových prostriedkov, sietí a dát prevádzkovaných ústavom.
- Kybernetický bezpečnostný incident – udalosť, ktorá ohrozuje alebo narušuje dôvernosť, integritu alebo dostupnosť informačných systémov.
- NAS (Network Attached Storage) – sieťové dátové úložisko slúžiace na zálohovanie a zdieľanie dát.
- VPN (Virtual Private Network) – šifrovaný vzdialený prístup do internej siete ústavu.
- Citlivé dáta – vedecké dáta, osobné údaje, finančné informácie a akékoľvek iné informácie, ktoré by ich neoprávnené zverejnenie mohlo spôsobiť škodu.
- Malvér – škodlivý softvér vrátane vírusov, ransomwaru, spywaru a iných hrozieb.
- Phishing – technika sociálneho inžinierstva za účelom získania citlivých informácií alebo prístupu k systémom.

Článok 3

Rozsah pôsobnosti a chránené priestory

(1) Táto smernica sa vzťahuje na všetkých používateľov informačných technológií ústavu bez ohľadu na ich pracovné zaradenie, vrátane externých spolupracovníkov a dodávateľov, ktorí majú prístup k systémom ústavu.

(2) Chránené priestory ústavu zahŕňajú:

- Serverovňa – miestnosť s centrálnymi servermi, prístupná výhradne správcovi IT a riaditeľovi ústavu. Vstup iných osôb je možný len v sprievode oprávnenej osoby. Serverovňa musí byť vybavená záložným zdrojom napájania (UPS).
- Kancelárie zamestnancov – prístup regulovaný na základe pracovného zaradenia; cudzie osoby vstupujú len v sprievode.
- Archívna miestnosť – uchovávanie fyzických nosičov dát a listinnej dokumentácie v uzamykateľných priestoroch.

(3) Pohyb osôb v chránených priestoroch:

- Vlastní zamestnanci – v rámci pridelených oprávnení a prístupových práv.
- Zamestnanci externých dodávateľov – výhradne pod dohľadom správcu IT alebo iného povereného zamestnanca.
- Upratovacia služba – nemá prístup do serverovne.

Článok 4

Politika používania informačných technológií

(1) Povinnosti správcu IT:

- Inštalácia, konfigurácia a správa operačných systémov a schválených aplikácií.
- Zriaďovanie, správa a rušenie používateľských kont a prístupových práv na základe žiadosti (vzor v Prílohe č. 1).
- Pravidelné zálohovanie systémových a používateľských dát.
- Monitorovanie stavu siete, serverov a bezpečnostných systémov.
- Vyhodnocovanie logovacích súborov serverov, firewallu a antivírusového systému.
- Správa antivírusového systému a zabezpečenie pravidelných aktualizácií.
- Riešenie kybernetických bezpečnostných incidentov a ich dokumentácia (Príloha č. 2).
- Vykonávanie bezpečnostných školení používateľov v spolupráci s bezpečnostným manažérom.
- Správa VPN a vzdialených prístupov.
- Pravidelná aktualizácia tejto bezpečnostnej dokumentácie.
- Hlásenie závažných bezpečnostných incidentov Národnému bezpečnostnému úradu (NBÚ) podľa § 22 zákona č. 69/2018 Z. z.

(2) Povinnosti každého používateľa:

- Dodržiavať túto smernicu a správať sa v súlade s ňou pri každej práci s IT zariadeniami ústavu.
- Informačné technológie používať výhradne na pracovné a výskumné účely ústavu.
- Po ukončení práce sa odhlásiť zo všetkých systémov a zamknúť pracovnú stanicu.
- Neotvárať prílohy z neznámych zdrojov a neklikáť na podozrivé prepojenia.
- Nesťahovať neschválený softvér, hry, video alebo zvukové súbory.
- Nikdy nezdieľať prihlasovacie meno a heslo s inou osobou.

- Bezodkladne hlásiť akýkoľvek bezpečnostný incident správcovi IT.
- Absolvovať bezpečnostné školenia v stanovených termínoch.
- Pri dlhšej neprítomnosti na pracovisku zabezpečiť uzamknutie obrazovky.

Článok 5

Používanie hardvéru

(1) Na pracovisku ústavu sa smie používať výhradne hardvér evidovaný v inventári ústavu a schválený riaditeľom alebo správcom IT.

(2) Zakazuje sa:

- Akákoľvek manipulácia, modifikácia alebo neoprávnená výmena hardvérových komponentov.
- Pripájanie neschválených zariadení (USB kľúče, externé disky, WiFi routery, mobilné prístupové body) bez predchádzajúceho súhlasu správcu IT.
- Pripájanie súkromných zariadení do internej siete ústavu bez výslovného súhlasu správcu IT.

(3) Zapožičané alebo pridelené mobilné zariadenia (notebooky, tablety):

- Zamestnanec je zodpovedný za ich bezpečné uchovávanie a zabraňuje ich strate, krádeži alebo zneužitiu.
- Zariadenia nesmú byť prenesené na tretiu osobu alebo zapožičané.
- Pri strate alebo krádeži je zamestnanec povinný bezodkladne informovať správcu IT a riaditeľa ústavu.

(4) Kľúčové servery sú umiestnené v serverovni a pripojené na záložný zdroj napájania (UPS). Na serveroch sa vykonávajú pravidelné aktualizácie a antivírusová kontrola podľa stanoveného harmonogramu.

(5) Poruchy hardvéru sa nahlásujú správcovi IT prostredníctvom interného systému hlásení. Správca IT zabezpečí opravu alebo výmenu v čo najkratšom čase.

Článok 6

Používanie softvéru

(1) Používatelia smú používať výhradne softvér nainštalovaný alebo schválený správcom IT. Inštaláciu nového softvéru vykonáva správca IT alebo poverená osoba.

(2) Zakazuje sa:

- Inštalovanie neschváleného, neautorizovaného alebo nelegálneho softvéru.
- Používanie softvéru na účely, na ktoré nebola udelená licencia.
- Sťahovanie softvéru z nedôveryhodných zdrojov.
- Deaktivácia alebo obchádzanie bezpečnostných programov (firewall, antivírus).

(3) Antivírusový softvér musí byť nainštalovaný na všetkých zariadeniach a musí sa automaticky aktualizovať. Správca IT zodpovedá za správu licencií a funkčnosť antivírusovej ochrany.

(4) Porucha softvéru sa nahlásuje správcovi IT. Dokumentácia poruchy a jej riešenie sa eviduje v internom systéme.

Článok 7

Používanie internetu a elektronickej pošty

(1) Pripojenie na internet je dostupné pre všetkých používateľov ústavu na pracovné a výskumné účely. Prístup na internet je monitorovaný a ústav má právo v súlade s platnou legislatívou preverovať použitie internetu a elektronickej pošty.

(2) Zakazuje sa:

- Používanie internetu a e-mailu na účely, ktoré porušujú platné právne predpisy SR a medzinárodné zmluvy.
- Sťahovanie a ukladanie nelegálneho softvéru, hier, video, obrázkov a zvukových súborov na zariadenia ústavu.
- Zobrazovanie, uchovávanie alebo rozširovanie obsahu s protiprávnym charakterom.
- Zámerné šírenie malvéru, vírusov alebo iného škodlivého softvéru.
- Vykonávanie útokov na iné počítačové systémy alebo siete.
- Zverejňovanie dôverných informácií o ústave na verejných platformách bez súhlasu riaditeľa.
- Prihlasovanie do webových aplikácií s možnosťou "Zostať prihlásený" na zariadeniach ústavu.

(3) Elektronická pošta:

- Používatelia nesmú otvárať prílohy z neznámych alebo podozrivých zdrojov.
- Phishingové e-maily alebo iné podozrivé správy je používateľ povinný bezodkladne nahlásiť správcovi IT a neodpovedať na ne.
- E-mail nesmie byť použitý na distribúciu dôverných informácií ústavu bez šifrovania.
- Ústav má právo nariadiť kontrolu obsahu e-mailov na zariadeniach ústavu v súlade s platnou legislatívou.

(4) Pre prístup z internetu do internej siete ústavu sa používa výhradne zabezpečená VPN.

(5) Cloudové služby a externé úložiská smú byť použité na pracovné účely len po schválení správcom IT a v súlade s politikou ochrany osobných údajov.

Článok 8

Správa prístupov a hesiel

(1) Každý používateľ dostane pridelené jedinečné prihlasovacie meno a heslo. Zdieľanie prihlasovacích údajov je prísne zakázané.

(2) Požiadavky na bezpečnosť hesla:

- Minimálna dĺžka: 12 znakov.
- Heslo musí obsahovať: aspoň 1 veľké písmeno, 1 malé písmeno, 1 číslicu a 1 špeciálny znak.
- Heslo nesmie obsahovať meno, priezvisko ani zjavné slovníkové slová.
- Heslo nesmie byť totožné s predchádzajúcimi 5 heslami.
- Platnosť hesla: odporúčaná výmena po 12 mesiacoch (v súlade so súčasnými bezpečnostnými odporúčaniami NIST a Microsoft); okamžitá výmena pri podozrení z kompromitácie.

(3) Pridelovanie a rušenie prístupov:

- Nový prístup sa prideliuje na základe žiadosti vedúceho pracovníka, schválenej riaditeľom (Príloha č. 1).
- Pri ukončení pracovného pomeru alebo zmene pracovnej pozície sa prístupové práva bezodkladne upravujú alebo zrušujú.
- Správca IT pravidelne (minimálne raz ročne) vykonáva revíziu aktívnych kont a prístupových práv.

(4) Správca IT a ďalší privilegovaní používatelia (s prístupom správcu) musia používať dvojfaktorovú autentifikáciu (2FA) pri prihlasovaní do kritických systémov.

(5) Pri odchode z pracoviska – aj krátkodobom – je používateľ povinný uzamknúť obrazovku pracovnej stanice (klávesová skratka Win+L alebo ekvivalent).

Článok 9

Zálohovanie a ochrana dát

(1) Zálohovanie dát je kľúčovým preventívnym opatrením. Správca IT zodpovedá za nastavenie a kontrolu zálohovania.

(2) Vedecké dáta projektov (výsledky meraní, datasety, raw data) sú považované za osobitne citlivé a zálohovanie podlieha požiadavkám príslušného projektového grantu a nariadení o riadení výskumných dát (DMP).

Článok 10

Narušenie bezpečnosti a riešenie incidentov

(1) Kybernetický bezpečnostný incident je akákoľvek udalosť, ktorá skutočne alebo potenciálne ohrozuje dôvernosť, integritu alebo dostupnosť informačných systémov ústavu.

(2) Každý používateľ je povinný bezodkladne nahlásiť správcovi IT akýkoľvek z nasledujúcich prípadov:

- Výskyt vírusu alebo malvéru na zariadení.
- Podozrenie na phishingový útok alebo sociálne inžinierstvo.
- Strata alebo krádež zariadenia s citlivými dátami.
- Neoprávnený prístup k systémom alebo dátam.
- Neobvyklé správanie zariadenia alebo aplikácie.
- Akýkoľvek iný podozrivý jav súvisiaci s IT bezpečnosťou.

(3) Postup pri riešení incidentu:

1. Okamžité izolovanie postihnutého zariadenia od siete (odpojenie sieťového kábla alebo vypnutie WiFi).
2. Nahlásenie incidentu správcovi IT a riaditeľovi ústavu.
3. Dokumentácia incidentu v Zázname o bezpečnostnom incidente (Príloha č. 2).
4. Analýza príčiny, rozsahu škody a možných dopadov.
5. Obnova systémov zo zálohy a obnovenie prevádzky.
6. Vyvodenie opatrení na predchádzanie opakovaniu.
7. V prípade závažného incidentu – hlásenie NBÚ do 24 hodín od zistenia, v súlade s § 22 zákona č. 69/2018 Z. z.

(4) Každý bezpečnostný incident musí byť zdokumentovaný. Dokumentácia sa uchováva minimálne 5 rokov.

(5) Porušenie mlčanlivosti alebo neoprávnený únik osobných údajov sa hlási Úradu na ochranu osobných údajov SR do 72 hodín od zistenia, v súlade s čl. 33 GDPR.

Článok 11

Preventívne opatrenia

(1) Technické preventívne opatrenia:

- Firewall – nastavený pre filtrovanie prevádzky; prístup z internetu obmedzený na nevyhnutné minimum.
- Antivírusová ochrana – inštalovaná na všetkých zariadeniach, automaticky aktualizovaná.
- Pravidelné bezpečnostné aktualizácie (patching) operačných systémov a aplikácií.
- Šifrovanie dát pri prenose citlivých informácií (TLS, VPN).
- Šifrovanie dát na mobilných zariadeniach (BitLocker alebo ekvivalent).
- Segmentácia siete – oddelenie administratívnej siete od výskumnej.
- Monitorovanie a logovanie sieťovej prevádzky a prístupov k systémom.
- Záložné zdroje napájania (UPS) pre kritické zariadenia.

(2) Organizačné preventívne opatrenia:

- Pravidelná revízia prístupových práv (minimálne 1x ročne).
- Princíp minimálnych oprávnení – používateľ má prístup len k systémom nevyhnutným pre výkon jeho práce.
- Fyzická bezpečnosť – uzamykanie kancelárií a serverovne.
- Kontrola a schvaľovanie externých dodávateľov s prístupom k systémom ústavu.
- Pravidlá čistého stola a čistej obrazovky – citlivé dokumenty sa neponechávajú bez dozoru.

Článok 12

Práca s citlivými a osobnými dátami

(1) Všetci zamestnanci sú povinní nakladať s citlivými dátami (vedecké dáta, osobné údaje, finančné informácie) tak, aby sa nedostali do rúk neoprávnených osôb.

(2) Bezpečnostné pravidlá pre prácu s citlivými dátami:

- Citlivé dáta sa nesmú ukladať na neschválené cloudové úložiská bez šifrovania.
- Prenosné médiá (USB) s citlivými dátami musia byť šifrované.
- Tlačené dokumenty s osobnými alebo citlivými údajmi sa po použití skartujú.
- Citlivé dáta sa nesmú zasielať e-mailom v nešifrovanej forme.
- Počítač sa nesmie nechať odomknutý bez dozoru na pracovisku prístupnom pre verejnosť.

(3) Likvidácia dát:

- Po uplynutí doby uchovávania sa osobné a citlivé dáta bezpečne likvidujú – elektronické dáta prepisom alebo fyzickým zničením média; listinné dokumenty skartovaním.
- Pevné disky a médiá z vyradených zariadení sa pred likvidáciou alebo ďalším použitím bezpečne vymažú.

(4) Povinnosť mlčanlivosti o citlivých dátach trvá aj po skončení pracovného pomeru.

Článok 13

Vzdelávanie a školenia

- (1) Všetci používatelia sú povinní absolvovať vstupné školenie o kybernetickej bezpečnosti a ochrane osobných údajov pri nástupe do pracovného pomeru alebo spolupráce s ústavom.
- (2) Opakované školenie sa vykonáva minimálne 1x ročne, alebo po závažnom bezpečnostnom incidente, alebo pri výraznej zmene právnych predpisov.
- (3) Správca IT a bezpečnostný manažér sú povinní sledovať aktuálny vývoj kybernetických hrozieb a pravidelne informovať zamestnancov o nových rizikách (napr. aktuálne phishingové kampane).
- (4) Účasť na školeniach sa eviduje. Odmietnutie účasti na školení sa považuje za porušenie tejto smernice.

Článok 14

Kontrola a audit

- (1) Správca IT vykonáva pravidelné kontroly stavu kybernetickej bezpečnosti:
 - Mesačne: prehľad logovacích súborov a bezpečnostných upozornení.
 - Štvrťročne: kontrola zálohovania a obnovy dát.
 - Polročne: revízia prístupových práv.
 - Ročne: celkový bezpečnostný audit, aktualizácia tejto smernice.
- (2) Ústav môže nariadiť mimoriadny audit v prípade bezpečnostného incidentu alebo podozrenia na porušenie bezpečnostných pravidiel.
- (3) Výsledky auditov sa predkladajú riaditeľovi ústavu a sú podkladom pre ďalšie opatrenia.

Článok 15

Záverečné ustanovenia

- (1) Porušenie povinností vyplývajúcich z tejto smernice sa považuje za porušenie pracovnej disciplíny a môže mať za následok disciplinárne konanie v súlade s Zákonníkom práce.
- (2) Závažné porušenia, ako napríklad zámerný únik citlivých dát, sabotáž systémov alebo inštalácia malvéru, môžu viesť k okamžitému skončeniu pracovného pomeru a trestnému oznámeniu.
- (3) Táto smernica nadobúda účinnosť dňom 1. 7. 2026.
- (4) Zrušuje sa akákoľvek predchádzajúca úprava kybernetickej bezpečnosti, ktorá je v rozpore s touto smernicou.
- (5) Smernica sa reviduje minimálne raz za 2 roky, alebo pri zmene relevantnej legislatívy.

Vypracoval:

Schválil:

Správca IT / Bezpečnostný manažér

Riaditeľka ústavu

Príloha č. 1 – Žiadosť o pridelenie prístupu do informačného systému

Meno a priezvisko žiadateľa:	
Pracovná pozícia:	
Oddelenie/Projekt:	
Požadovaný prístup:	
Odôvodnenie požiadavky:	
Platnosť prístupu (od – do):	
Podpis žiadateľa:	
Schválenie vedúceho:	
Pridelil správca IT:	

Príloha č. 2 – Záznam o bezpečnostnom incidente

Dátum a čas incidentu:	
Kto incident hlásil:	
Postihnuté systémy/zariadenia:	
Popis incidentu:	
Typ incidentu:	☐ Malvér ☐ Phishing ☐ Neoprávnený prístup ☐ Únik dát ☐ Iné: _____
Závažnosť:	☐ Nízka ☐ Stredná ☐ Vysoká ☐ Kritická
Prijaté opatrenia:	
Hlásenie NBÚ:	☐ Áno – dátum: _____ ☐ Nie
Incident uzavretý (dátum):	
Podpis správcu IT:	